

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
10. Mai 2002 (10.05.2002)

PCT

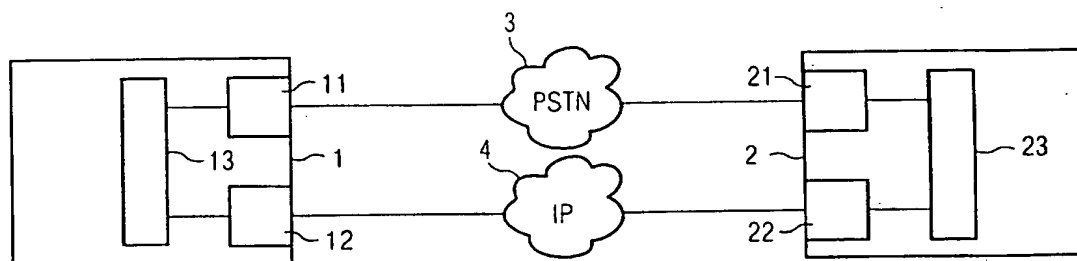
(10) Internationale Veröffentlichungsnummer
WO 02/37745 A1

- (51) Internationale Patentklassifikation⁷: **H04L 9/00.** (74) **Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT;** Postfach 22 16 34, 80506 München (DE).
- (21) Internationales Aktenzeichen: **PCT/DE01/04167**
- (22) Internationales Anmeldedatum:
6. November 2001 (06.11.2001)
- (25) Einreichungssprache: **Deutsch**
- (26) Veröffentlichungssprache: **Deutsch**
- (30) Angaben zur Priorität:
100 54 941.1 6. November 2000 (06.11.2000) **DE**
- (71) **Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): SIEMENS AKTIENGESELLSCHAFT [DE/DE];** Wittelsbacherplatz 2, 80333 München (DE).
- (72) **Erfinder: und**
- (75) **Erfinder/Anmelder (nur für US): FRISCH, Norbert [DE/DE];** Bertha von Suttner Weg 16, 82152 Martinsried (DE).
- (81) **Bestimmungsstaaten (national):** BR, CN, US.
- (84) **Bestimmungsstaaten (regional):** europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- Erklärungen gemäß Regel 4.17:**
- hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten BR, CN, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR)
 - Erfindererklärung (Regel 4.17 Ziffer iv) nur für US
- Veröffentlicht:**
- mit internationalem Recherchenbericht
 - vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR SECURELY TRANSMITTING DATA BETWEEN TWO TERMINALS AND A CORRESPONDING DEVICE FOR CARRYING OUT THIS METHOD

(54) **Bezeichnung:** VERFAHREN ZUR SICHEREN DATENÜBERTRAGUNG ZWISCHEN ZWEI ENDGERÄTEN UND VORRICHTUNG ZUR DURCHFÜHRUNG DIESES VERFAHRENS



(57) **Abstract:** The invention relates to a method for securely transmitting data between two terminals (1, 2), whereby security-relevant data and useful data are transmitted. The security-relevant data is transmitted between the terminals (1, 2) over a first data transmission network (3), and the useful data is transmitted between the terminals (1, 2) over a second data transmission network (4). The invention also relates to a terminal (1, 2) for carrying out this method.

(57) **Zusammenfassung:** Die vorliegende Erfindung betrifft ein Verfahren zur Datenübertragung zwischen zwei Endgeräten (1, 2), wobei sicherheitsrelevante Daten und Nutzdaten übertragen werden, die sicherheitsrelevanten Daten über ein erstes Datenübertragungsnetz (3) und die Nutzdaten über ein zweites Datenübertragungsnetz (4) zwischen den Endgeräten (1, 2) übertragen werden. Weiterhin betrifft die vorliegende Erfindung ein Endgerät (1, 2) zur Durchführung dieses Verfahrens.

WO 02/37745 A1



Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zur sicheren Datenübertragung zwischen zwei Endgeräten und Vorrichtung zur Durchführung dieses Verfahrens

5

Die vorliegende Erfindung betrifft ein Verfahren zur sicheren Datenübertragung zwischen zwei Endgeräten und eine Vorrichtung zur Durchführung dieses Verfahrens.

- 10 Werden Daten zwischen zwei Teilnehmern bzw. deren Endgeräten über ein Datenübertragungsnetz übertragen, das nicht sicher ist, so müssen die Daten verschlüsselt werden. Ein Beispiel hierfür ist die Datenübertragung zwischen einem Kunden (erster Teilnehmer) und seiner Bank (zweiter Teilnehmer) über das
- 15 Internet, wobei der Kunde die Möglichkeit hat, über das Internet Bankgeschäfte abzuwickeln.

- Das Internet bietet jedoch keine sichere Datenübertragung, d.h. ein Dritter hat die Möglichkeit, die Daten während der
- 20 Datenübertragung "abzuhören". Bei der Übertragung von sicherheitsrelevanten Daten, wie z.B. Zugangskennung, PIN-Nummer und Kontonummer, könnte somit ein unbefugter Zugriff durch einen Dritten auf das jeweilige Konto erfolgen. Zur Übertragung von Daten, die sicherheitsrelevante Daten enthalten,
- 25 müssen die zu übertragenden Daten von dem Versenden verschlüsselt und beim Empfangen wieder entschlüsselt werden.

- Das gleiche gilt auch für die Datenübertragung beispielsweise via E-Mail, wenn es sich bei den zu übertragenden Daten um
- 30 vertrauliche Daten handelt.

Zur Verschlüsselung sind zwei Arten von Verfahren bekannt: die symmetrische und die asymmetrische Verschlüsselung.

- 35 Bei der symmetrischen Verschlüsselung werden die zu übertragenden Daten mit einem bestimmten Schlüssel (Code) verschlüsselt. Die Entschlüsselung der Daten erfolgt durch den Empfänger.

ger mit dem gleichen Schlüssel. Da beide Teilnehmer somit den gleichen Schlüssel besitzen müssen, ist dieses Verfahren relativ unsicher, wenn der Schlüssel von einem Teilnehmer zu einem anderen Teilnehmer übertragen wird und sich beispielsweise bei der Übertragung des Schlüssels ein unbefugter Dritter diesen Schlüssel aneignet.

Bei der asymmetrischen Verschlüsselung, wie es beispielsweise im PGP-Verfahren (Pretty Good Privacy) angewendet wird, werden die zu übertragenden Daten mit einem sogenannten öffentlichen Schlüssel durch den Sender verschlüsselt und mit einem sogenannten privaten Schlüssel durch den Empfänger entschlüsselt. Der öffentliche Schlüssel kann dabei jederman zugänglich gemacht werden, während der private Schlüssel nur dem Empfänger bekannt ist. Dieses Verfahren ist gegenüber dem symmetrischen Verschlüsselungsverfahren erheblich sicherer, da der private Schlüssel nicht versendet werden muß und somit nur dem Empfänger bekannt ist. Der Nachteil dieses Verschlüsselungsverfahrens ist jedoch, daß es wesentlich umständlicher ist: Es muß zuerst ein Schlüsselpaar (öffentlicher und privater Schlüssel) generiert werden. Dann muß der öffentliche Schlüssel für andere Teilnehmer zugänglich gemacht werden, d.h. der öffentliche Schlüssel wird dabei beispielsweise öffentlich zugänglich auf einem Internet-Server abgelegt oder an die jeweiligen Partner versendet.

Die Aufgabe der vorliegenden Erfindung ist somit, ein Verfahren zur Datenübertragung zwischen zwei Endgeräten und ein Endgerät zur Durchführung dieses Verfahrens bereitzustellen, bei denen eine Datenübertragung zwischen zwei Teilnehmern bzw. deren Endgeräten ermöglicht wird, die, in Bezug auf unbefugte Zugriffe durch Dritte, sicher ist und bei denen die sichere Datenübertragung für Anwender vereinfacht wird.

Diese Aufgabe wird durch ein Verfahren zur Datenübertragung zwischen zwei Endgeräten gemäß dem beigefügten Anspruch 1 und

ein Endgerät zur Durchführung dieses Verfahrens gemäß dem beigefügten Anspruch 6 gelöst.

5 Gemäß der vorliegenden Erfindung erfolgt die Datenübertragung für eine Anwendung zwischen zwei Endgeräten über zwei separate Datenübertragungsnetze (erstes und zweites Datenübertragungsnetz), wobei über das erste Datenübertragungsnetz sicherheitsrelevante Daten und über das zweite Datenübertragungsnetz zugehörige Nutzdaten übertragen werden.

10

Zusammengehörende sicherheitsrelevante Daten und Nutzdaten sind z.B. Daten, die zum Durchführen einer Anwendung (z.B. die Eingangs beschriebene "Bankanwendung") zwischen zwei Endgeräten übertragen werden.

15

Vorteilhafte Ausgestaltungen der vorliegenden Erfindung sind in den jeweiligen Unteransprüchen wiedergegeben.

20 Damit die sicherheitsrelevanten Daten für Unbefugte unzugänglich (d.h. sicher) übertragen werden, werden diese Daten vorteilhafterweise über eine sichere Verbindung übertragen. Eine sichere Verbindung stellt dabei das öffentliche Fernsprechnetz (PSTN, Public Switched Telephone Network im analog- oder ISDN-Verfahren) zur Verfügung, das ein leitungsvermittelltes
25 Datenübertragungsnetz ist und eine sichere Punkt-zu-Punkt-Verbindung zur Datenübertragung zwischen zwei Teilnehmern herstellt.

30 Sicherheitsrelevante Daten können z.B. Zugangsdaten, PIN-Nummern (Personal Identification Number), Kontonummern, usw. sein, die beispielsweise den Zugriff auf ein Konto bei einer Bank freigeben und die Durchführung von Bankgeschäften zu diesem Konto ermöglichen.

35 Daten, die nicht sicherheitsrelevant sind (Nutzdaten), können beispielsweise Text- und/oder Formatierungsinformationen usw. sein, die keine vertraulichen Daten beinhalten.

So kann z.B. über das zweite Datenübertragungsnetz ein Text übertragen werden, der anstatt sicherheitsrelevanter Daten Lücken enthält. Diese Lücken werden mit den sicherheitsrelevanten Daten (vertrauliche Daten), die über das erste Datenübertragungsnetz übertragen werden, ausgefüllt.

Weiterhin können die sicherheitsrelevanten Daten auch Verschlüsselungscodes beinhalten, mit denen die Nutzdaten, die über das zweite Datenübertragungsnetz übertragen werden, verschlüsselt bzw. entschlüsselt werden.

In diesem Fall können auch geheime Daten, wie z.B. PIN-Nummern und andere Daten, die keinem Dritten zugänglich gemacht werden dürfen, über das zweite Datenübertragungsnetz übertragen werden, da diese Daten mit einem Verschlüsselungscodeweg (erstes Datenübertragungsnetz) als die Nutzdaten (zweites Datenübertragungsnetz) übertragen wird.

Die Nutzdaten, die in der Regel einen wesentlich größeren Anteil an zu übertragenden Daten ausmachen als die sicherheitsrelevanten Daten, werden weiterhin über ein nicht sicheres breitbandiges (zweites) Datenübertragungsnetz, z.B. dem Internet, das ein paketvermitteltes Datenübertragungsnetz ist, übertragen.

Bei entsprechender Anforderung an die Sicherheit können die sicherheitsrelevanten Daten zusätzlich noch verschlüsselt über das erste Datenübertragungsnetz übertragen werden.

Die Trennung der zu übertragenden Daten in sicherheitsrelevante Daten und Nutzdaten erfolgt durch die Einrichtung (13, 23) zum automatischen Auftrennen bzw. Zusammenführen von Daten automatisch nach voreingestellten Kriterien. So können beispielsweise bestimmte Felder in einem Formular als sicherheitsrelevant gekennzeichnet werden. Solche Felder sind z.B.

Felder zur Eingabe von PIN (Personal Identification Number, TAN (Transaktionsnummer), Kontonummer, Betrag, Zugangsdaten, usw.

- 5 Einer weitere Möglichkeit, die erfindungsgemäße Trennung der Daten vorzunehmen, besteht darin, generell alle vorkommenden Zahlen als sicherheitsrelevant einzustufen und über das erste Datenübertragungsnetz zu übertragen.
- 10 Wie bereits beschrieben, können über das erste Datenübertragungsnetz auch Verschlüsselungsdaten zur Ver- bzw. Entschlüsselung der Nutzdaten übertragen werden. Somit werden die Verschlüsselungsdaten (Codes) als sicherheitsrelevant definiert und über das erste Datenübertragungsnetz übertragen. Alle an-
- 15 deren Daten, einschließlich von Zugangsdaten, PIN-Nummern, usw., sind, da sie verschlüsselt sind, als Nutzdaten definiert und werden dementsprechend über das zweite Datenübertragungsnetz übertragen.
- 20 Der Vorteil der vorliegenden Erfindung besteht in der besonders einfachen Handhabung für die Nutzer einer gesicherten Datenübertragung. Weiterhin wird die Sicherheit der Datenübertragung durch die gleichzeitige Verwendung von zwei Datenübertragungsnetzen erhöht, insbesondere mit der Verwendung
- 25 des öffentlichen Fernsprechnetzes, das eine sichere Punkt-zu-Punkt-Verbindung bereitstellt, als erstes Datenübertragungsnetz.

Die vorliegende Erfindung wird nachfolgend anhand bevorzugter

30 Ausführungsbeispiele unter Bezug auf die beigefügten Zeichnungen näher erläutert, in denen zeigen:

Fig. 1 eine schematische Darstellung einer Datenübertragung zwischen zwei erfindungsgemäßen Endgeräten unter Anwendung

35 des erfindungsgemäßen Verfahrens,

Fig. 2 eine schematische Darstellung der erfindungsgemäßen Datenübertragung im xDSL-Übertragungssystem, und

5 Fig. 3 eine schematische Darstellung der erfindungsgemäßen Datenübertragung über unterschiedliche Zugänge zu den Datenübertragungsnetzen.

10 Anhand von Fig. 1 wird nachfolgend die Funktionsweise der vorliegenden Erfindung anhand einer "Bankanwendung" näher erläutert, wobei eine beispielhafte Datenübertragung zwischen einem Kunden und seiner Bank stattfindet.

15 Der Kunde stellt dabei mit seinem PC (Endgerät 1) über das Internet (IP, zweites Datenübertragungsnetz 4) eine Verbindung mit dem Bankrechner (Endgerät 2) her.

20 Gemäß der vorliegenden Erfindung werden zur Erhöhung der Sicherheit bei der Datenübertragung gleichzeitig zwei Datenübertragungsnetze (erstes und zweites Datenübertragungsnetz 3, 4) zur Datenübertragung genutzt. Dabei werden über das Internet Massendaten (Nutzdaten) übertragen, die keine sicherheitsrelevanten Informationen enthalten, wie z.B. Text, Formatierungs- und Layout-Informationen.

25 Über das öffentliche Fernsprechnetz werden sicherheitsrelevante Daten übertragen, wie z.B. Zugangskennungen, PIN-Nummern, Kontonummern, usw. für den Zugriff auf das jeweilige Konto. Weiterhin können die sicherheitsrelevanten Daten auch Verschlüsselungsdaten (Verschlüsselungscode) zur Ver- bzw.
30 Entschlüsselung der Nutzdaten, die über das zweite Datenübertragungsnetz übertragen werden, beinhalten.

35 Soll eine sichere Verbindung zwischen zwei Endgeräten 1 und 2 (z.B. PC eines Kunden mit Bankrechner) aufgebaut werden, so wird durch die jeweilige Einrichtung 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten zusätzlich zur Datenübertragung über das Internet eine Verbindung über das öf-

fentliche Fernsprechnetz aufgebaut; die jeweiligen Verbindungen erfolgen mittels der ersten und zweiten Schnittstelle 11, 21 und 12, 22 Die Einrichtung 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten beinhaltet eine entsprechende Applikationssoftware, die die notwendigen Signalisierungsaufgaben zum Aufbau, zur Steuerung und zum Abbau der Verbindungen durchführt. Diese Applikationssoftware nimmt auch beim Senden eine Trennung und beim Empfangen eine Zusammenführung vom sicherheitsrelevanten Daten und Nutzdaten vor.

10

Zu den getrennten Daten werden durch die Applikationssoftware beim Senden Informationen hinzugefügt, die eine Rekonstruktionsreihenfolge oder einen Rekonstruktionsalgorithmus beinhalten. Anhand dieser Reihenfolge (im einfachsten Fall eine Durchnumerierung von Datenpaketen) bzw. dieses Algorithmus werden durch die empfangende Einrichtung 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten die Daten wieder in der richtigen Reihenfolge zusammengesetzt. Gegebenenfalls werden auch die Nutzdaten durch die empfangende Einrichtung 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten entschlüsselt.

15
20

Anhand von Fig. 2 wird nachfolgend die Implementierung der vorliegenden Erfindung im xDSL-Übertragungsverfahren (x Digital Subscriber Line) erläutert.

25

Im xDSL-Übertragungsverfahren erfolgt die Datenübertragung in verschiedenen Frequenzbändern. Die Übertragung der (sicherheitsrelevanten) Daten, die über das öffentliche Fernsprechnetz 3 (PSTN) im POTS (Plain Old Telephone Service) oder ISDN (Integrated Services Digital Network) übertragen werden, werden von den Endgeräten 1, 2 in einem tiefen (relativ kleinen) Frequenzband übertragen (beispielsweise 0 bis 32 kHz). Die Daten, die über das Internet 4 (IP) übertragen werden, werden in einem breiteren, oberhalb von 32 kHz liegenden Frequenzband von den Endgeräten 1, 2 übertragen. Die Datenübertragung

30
35

beider Frequenzbänder erfolgt dabei von bzw. zu den Endgeräten 1, 2 über eine physikalische Leitung.

Im Beispiel von Fig. 2 besteht die Aufgabe der ersten und zweiten Schnittstellen 11, 21 und 12, 22 der jeweiligen Endgeräte 1, 2 somit darin, die sicherheitsrelevanten Daten und die Nutzdaten zum Senden in die entsprechenden Frequenzbänder zu transformieren (in dieser Figur durch das Tief- bzw. durch das Hochpaßsymbol dargestellt) und die Daten auf einer gemeinsamen physikalischen Leitung zu versenden. Beim Empfangen von Daten erfolgt umgekehrt eine Trennung der Frequenzbänder durch die jeweilige erste bzw. zweite 11, 21 bzw. 12, 22 Schnittstelle. Die Verarbeitung der Daten erfolgt, wie bereits anhand von Fig. 1 beschrieben, anhand der jeweiligen Einrichtung 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten.

Die Daten, die über eine physikalische Leitung in verschiedenen Frequenzbändern übertragen werden, müssen zum Versenden über die unterschiedlichen Übertragungsnetze auf diese Netze aufgeteilt werden. Zum Empfangen werden die Daten wiederum über eine Leitung in unterschiedlichen Frequenzbändern zum Endgerät übertragen.

Diese Aufgaben werden durch sogenannte xDSL-Splitter bzw. xDSL-Merger (in der Fig. 2 mit den Bezugszeichen 5 und 6 bezeichnet) durchgeführt, je nachdem, ob die Daten versendet oder empfangen werden.

Diese xDSL-Splitter/Merger befinden sich physikalisch vor der Vermittlungsstelle; sie können aber auch Bestandteil der Vermittlungsstelle sein. Zum Versenden von Daten nehmen sie eine Aufteilung der Daten entsprechend dem Frequenzband vor und versenden die Daten über das entsprechende Datenübertragungsnetz. Zum Empfangen werden die Daten aus den jeweiligen Datenübertragungsnetzen in die entsprechenden Frequenzbänder transformiert und zum jeweiligen Endgerät 1, 2 übertragen.

Anhand von Fig. 3 wird die erfindungsgemäße Datenübertragung bei beliebigen Zugängen zum Internet und zum öffentlichen Fernsprechnetzt erläutert.

5

Der Zugang der Endgeräte 1, 2 zum Internet kann z.B. über eine sogenannte Powerline, d.h. über Stromkabel, oder einem anderen Breitbandkabel (z.B. Fernseekabel) erfolgen. Die Endgeräte 1, 2 müssen zu diesem Zweck entsprechende zweite
10 Schnittstellen 12 und 22 aufweisen. Bei der Übertragung von sicherheitsrelevanten Daten wird zwischen den jeweiligen Einrichtungen 13, 23 zum automatischen Auftrennen bzw. Zusammenführen von Daten eine Verbindung über die ersten Schnittstellen 11, 21 aufgebaut. Im gezeigten Beispiel folgt der Zugang
15 von Endgerät 1 zum öffentlichen Fernsprechnetzt über eine Mobilfunkschnittstelle (GSM) und von Endgerät 2 über das Festnetz.

Dabei sind alle sich daraus ergebenden Zugangsmischformen
20 denkbar, d.h. daß das Endgerät 1 andere Zugänge zu den beiden Datenübertragungsnetzen haben kann als das Endgerät 2.

Die vorliegende Erfindung findet überall dort Anwendung, wo eine gesicherte Datenübertragung, d.h. eine Datenübertragung,
25 die gegen unautorisierte Zugriffe geschützt werden soll, stattfindet.

Neben der beschriebenen Anwendung zur Abwicklung von Bankgeschäften sind auch weitere Anwendungen im gesamten E-Commerce
30 und Multimediabereich denkbar: So können z.B. bei Video-on-demand, bei dem Filme von einem Teilnehmer individuell abgerufen werden können, die codierten Nutzdaten (Video) über das Internet empfangen werden. Der jeweilige Teilnehmer erhält den aktuell bezahlten Schlüssel zur Dekodierung dieses Films
35 über das sichere öffentliche Fernsprechnetzt. Das gleiche gilt für jede beliebige Bild-, Ton- und Filmübertragung. Die Übertragung der Nutzdaten muß dabei nicht über das Internet er-

folgen, es ist auch ein beliebiges anderes Breitbandnetz denkbar.

5 Die vorliegende Erfindung läßt sich auch für die Abwicklung von allen Arten von Geschäften (z.B. B2B, Business-to-Business) über das Internet anwenden. Dabei werden die wesentlichen Geschäftsdaten, die z.B. auch eine sog. digitale Signatur für die Echtheitszertifizierung enthalten, automatisch über das sichere Fernsprechnetz übertragen.

Patentansprüche

1. Verfahren zur Datenübertragung zwischen zwei Endgeräten
(1, 2), wobei sicherheitsrelevante Daten und zugehörige Nutz-
5 daten übertragen werden,
dadurch gekennzeichnet,
daß die sicherheitsrelevanten Daten über ein erstes Daten-
übertragungsnetz (3) und die Nutzdaten über ein separates
zweites Datenübertragungsnetz (4) zwischen den Endgeräten (1,
10 2) übertragen werden.
2. Verfahren gemäß Anspruch 1,
dadurch gekennzeichnet,
daß das erste Datenübertragungsnetz (3) ein leitungsvermit-
15 teltes Datenübertragungsnetz und das zweite Datenübertra-
gungsnetz (4) ein paketvermitteltes Datenübertragungsnetz
ist.
3. Verfahren gemäß Anspruch 1 oder 2,
20 dadurch gekennzeichnet,
daß die sicherheitsrelevanten Daten und die Nutzdaten zeit-
gleich übertragen werden.
4. Verfahren gemäß Anspruch 1, 2 oder 3,
25 dadurch gekennzeichnet,
daß die sicherheitsrelevanten Daten Zugangsdaten für eine be-
stimmte Anwendung sind.
5. Verfahren gemäß einem der Ansprüche 1 bis 4,
30 dadurch gekennzeichnet,
daß die sicherheitsrelevanten Daten Verschlüsselungsdaten zur
Verschlüsselung der Nutzdaten beinhalten.
6. Endgerät (1, 2) zur Durchführung des Verfahrens gemäß ei-
35 nem der Ansprüche 1 bis 5, mit
einer ersten Schnittstelle (11, 21) zur Datenübertragung über
ein erstes Datenübertragungsnetz (3),

einer zweiten Schnittstelle (12, 22) zur Datenübertragung über ein zweites Datenübertragungsnetz (4), und einer Einrichtung (13, 23) zum automatischen Auftrennen bzw. Zusammenführen von sicherheitsrelevanten Daten des ersten Datenübertragungsnetzes (3) und Nutzdaten des zweiten Datenübertragungsnetzes (4) mittels der ersten und zweiten Schnittstelle.

7. Endgerät (1, 2) gemäß Anspruch 6, dadurch gekennzeichnet, daß die Einrichtung (13, 23) zum automatischen Auftrennen bzw. Zusammenführen von Daten die Trennung bzw. Zusammenführung nach voreingestellten Kriterien vornimmt.

8. Endgerät (1, 2) gemäß Anspruch 7, dadurch gekennzeichnet, daß die Einrichtung (13, 23) zum automatischen Auftrennen bzw. Zusammenführen automatisch Zahlen als sicherheitsrelevant definiert, während sie alle anderen Daten als Nutzdaten definiert.

9. Endgerät (1, 2) gemäß Anspruch 7, dadurch gekennzeichnet, daß Einrichtung (13, 23) zum automatischen Auftrennen bzw. Zusammenführen Daten, die in speziell gekennzeichneten Formularfeldern enthalten sind, automatisch als sicherheitsrelevant definiert, während sie alle anderen Daten als Nutzdaten definiert.

10. Endgerät (1, 2) gemäß einem der Ansprüche 6 bis 9, dadurch gekennzeichnet, daß die erste Schnittstelle (11, 21) die Datenübertragung über ein Leitungvermitteltes Datenübertragungsnetz und die zweite Schnittstelle (12, 22) die Datenübertragung über ein paketvermitteltes Datenübertragungsnetz durchführt.

1/2

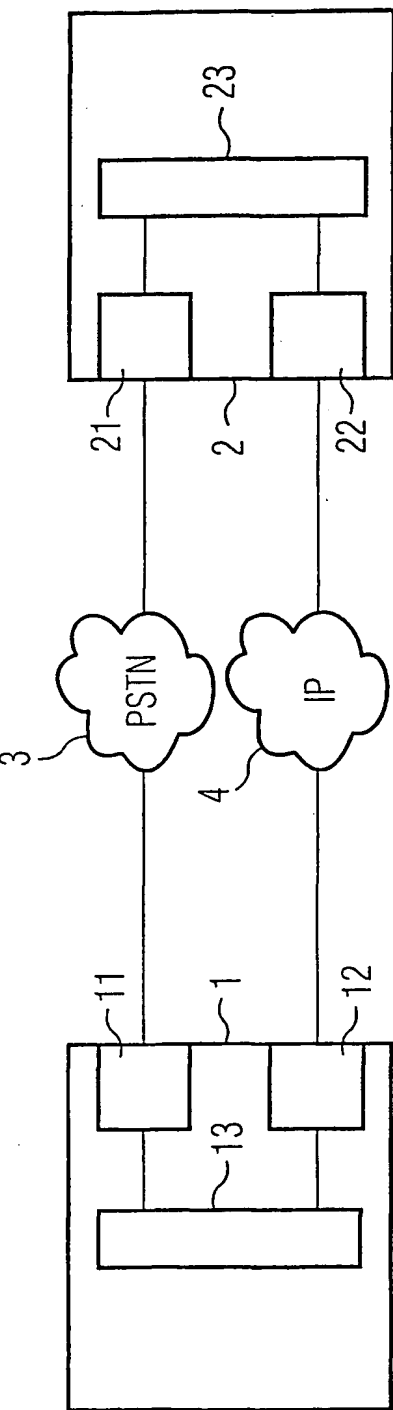


FIG 1

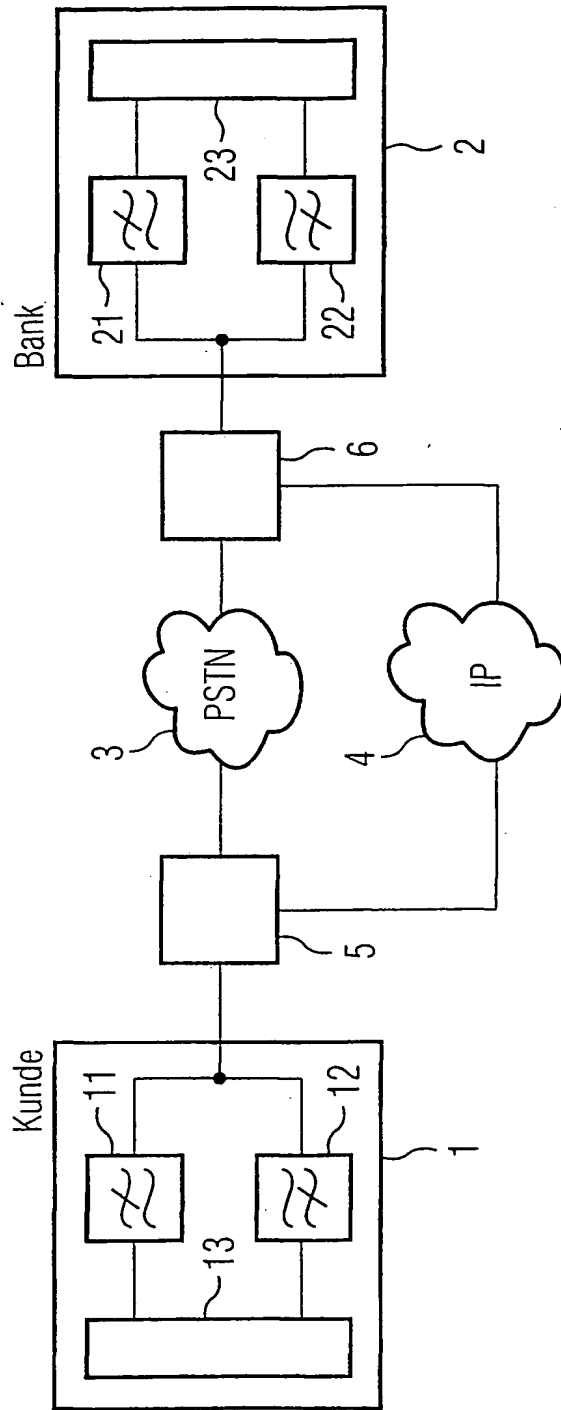
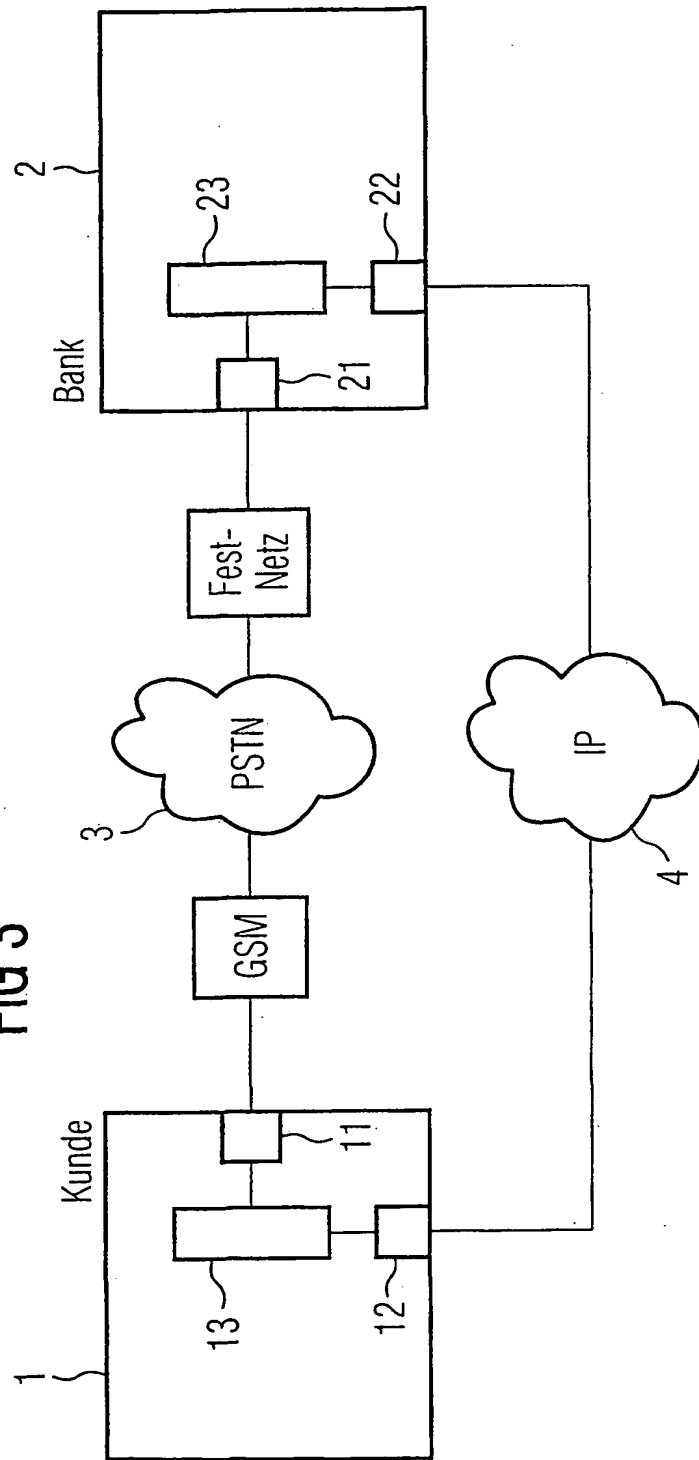


FIG 2

2/2

FIG 3



INTERNATIONAL SEARCH REPORT

International Application No

PCT/DE 01/04167

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/00 H04L29/06 H04L9/08 H04L9/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 869 651 A (ERICSSON TELEFON AB L M) 7 October 1998 (1998-10-07) abstract column 4, line 4 - line 30 column 5, line 2 - column 6, line 26; figures 1-3	1-10
X	EP 0 801 479 A (AT & T CORP) 15 October 1997 (1997-10-15) column 5, line 8 - line 48 column 7, line 15 - column 8, line 29; figures 1-4	1-10
X	US 6 012 144 A (PICKETT THOMAS E) 4 January 2000 (2000-01-04) abstract column 3, line 43 - column 4, line 54 column 7, line 1 - line 5; figures 1,2	1-10
	--- -/--	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

* & * document member of the same patent family

Date of the actual completion of the international search

28 February 2002

Date of mailing of the international search report

06/03/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Buhleier, R

INTERNATIONAL SEARCH REPORT

International Application No

PCT/DE 01/04167

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 926 611 A (AT & T CORP) 30 June 1999 (1999-06-30)	1,2,4
A	paragraph '0018!; figure 1 ---	3,5-10
A	BONNEY J C ET AL: "Universal broadband network access device" PARALLEL ARCHITECTURES, ALGORITHMS, AND NETWORKS, 1996. PROCEEDINGS., SECOND INTERNATIONAL SYMPOSIUM ON BEIJING, CHINA 12-14 JUNE 1996, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 12 June 1996 (1996-06-12), pages 146-153, XP010166771 ISBN: 0-8186-7460-1 page 148, right-hand column, paragraph 4 -page 149, left-hand column, paragraph 5; figure 1 ---	6
A	JACKSON A: "ADSL for high-speed broadband data service" AEROSPACE CONFERENCE, 1998 IEEE SNOWMASS AT ASPEN, CO, USA 21-28 MARCH 1998, NEW YORK, NY, USA, IEEE, US, 21 March 1998 (1998-03-21), pages 451-465, XP010286910 ISBN: 0-7803-4311-5 page 454, right-hand column, paragraph 5 -page 456, right-hand column, last paragraph; figures 3-7 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 01/04167

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0869651	A	07-10-1998	WO 9844693 A1	08-10-1998
			EP 0869651 A1	07-10-1998
			AU 6632598 A	22-10-1998
			JP 2001517396 T	02-10-2001
			NO 994221 A	30-09-1999
			US 6199165 B1	06-03-2001
EP 0801479	A	15-10-1997	US 6252869 B1	26-06-2001
			CA 2193748 A1	30-06-1997
			EP 0801479 A1	15-10-1997
			JP 10031634 A	03-02-1998
US 6012144	A	04-01-2000	NONE	
EP 0926611	A	30-06-1999	EP 0926611 A2	30-06-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 01/04167

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 H04L9/00 H04L29/06 H04L9/08 H04L9/12

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, INSPEC, IBM-TDB, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Beir. Anspruch Nr.
X	EP 0 869 651 A (ERICSSON TELEFON AB L M) 7. Oktober 1998 (1998-10-07) Zusammenfassung Spalte 4, Zeile 4 - Zeile 30 Spalte 5, Zeile 2 - Spalte 6, Zeile 26; Abbildungen 1-3	1-10
X	EP 0 801 479 A (AT & T CORP) 15. Oktober 1997 (1997-10-15) Spalte 5, Zeile 8 - Zeile 48 Spalte 7, Zeile 15 - Spalte 8, Zeile 29; Abbildungen 1-4	1-10



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

I Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

& Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

28. Februar 2002

Absendedatum des internationalen Recherchenberichts

06/03/2002

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Buhleier, R

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 01/04167

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Beitr. Anspruch Nr.
X	US 6 012 144 A (PICKETT THOMAS E) 4. Januar 2000 (2000-01-04) Zusammenfassung Spalte 3, Zeile 43 - Spalte 4, Zeile 54 Spalte 7, Zeile 1 - Zeile 5; Abbildungen 1,2 ----	1-10
X	EP 0 926 611 A (AT & T CORP) 30. Juni 1999 (1999-06-30)	1,2,4
A	Absatz '0018!; Abbildung 1 ----	3,5-10
A	BONNEY J C ET AL: "Universal broadband network access device" PARALLEL ARCHITECTURES, ALGORITHMS, AND NETWORKS, 1996. PROCEEDINGS., SECOND INTERNATIONAL SYMPOSIUM ON BEIJING, CHINA 12-14 JUNE 1996, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 12. Juni 1996 (1996-06-12), Seiten 146-153, XP010166771 ISBN: 0-8186-7460-1 Seite 148, rechte Spalte, Absatz 4 -Seite 149, linke Spalte, Absatz 5; Abbildung 1 ----	6
A	JACKSON A: "ADSL for high-speed broadband data service" AEROSPACE CONFERENCE, 1998 IEEE SNOWMASS AT ASPEN, CO, USA 21-28 MARCH 1998, NEW YORK, NY, USA, IEEE, US, 21. März 1998 (1998-03-21), Seiten 451-465, XP010286910 ISBN: 0-7803-4311-5 Seite 454, rechte Spalte, Absatz 5 -Seite 456, rechte Spalte, letzter Absatz; Abbildungen 3-7 -----	

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 01/04167

Im Recherchenbericht angeführtes Patentedokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0869651	A	07-10-1998	WO 9844693 A1	08-10-1998
			EP 0869651 A1	07-10-1998
			AU 6632598 A	22-10-1998
			JP 2001517396 T	02-10-2001
			NO 994221 A	30-09-1999
			US 6199165 B1	06-03-2001
EP 0801479	A	15-10-1997	US 6252869 B1	26-06-2001
			CA 2193748 A1	30-06-1997
			EP 0801479 A1	15-10-1997
			JP 10031634 A	03-02-1998
US 6012144	A	04-01-2000	KEINE	
EP 0926611	A	30-06-1999	EP 0926611 A2	30-06-1999